

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF WEST VIRGINIA
MARTINSBURG**

**IN THE MATTER OF THE SEARCH OF
TEN ELECTRONIC DEVICES SEIZED
FROM 721 FAULKNER AVENUE,
MARTINSBURG, WEST VIRGINIA ON
JANUARY 19, 2023**

Case No. 3:23-mj-8

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Ellen Duffy, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and I have been so employed since January 2018. Prior to my employment with the FBI, I was employed with the University of Florida Police Department (UFPD) for approximately seven years. During my employment with UFPD, I served as a Patrol Officer, a Detective, and a Detective Sergeant. Prior to my employment with UFPD, I was employed as a Special Agent with the United States Department of Education, Office of Inspector General for approximately two years. I am currently assigned to a multi-agency task force known as the West Virginia Child Exploitation and Human Trafficking Task Force (WVCEHTTF). Since June 2018, my responsibilities in the FBI have included the enforcement of federal criminal statutes involving the sexual exploitation of children pursuant to Title 18, United States Code, Section 2422, et seq. I have received training regarding the Internet, online child pornography, child exploitation, and child sex trafficking, and have consulted with my colleagues who have many years of experience investigating child exploitation cases. I have also been the affiant on

numerous prior search and arrest warrants. As a federal agent, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with the authority to execute arrest and search warrants issued under the authority of the United States.

2. I make this affidavit in support of an application for a search warrant for ten electronic devices seized from 721 Faulkner Avenue, Martinsburg, West Virginia on January 19, 2023 (“the TARGET DEVICES”), further described in Attachment A.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 2251(a) (Production of Child Pornography), 2252A(a)(2)(B) (Distribution of Child Pornography), 2252A(a)(5)(B) (Possession of Child Pornography), and 1591(a) (Sex Trafficking of Children) have been committed by Destiny Somersall, John Balch, and other yet-to-be identified subjects, from approximately November 2020 through January 19, 2023. There is also probable cause to believe the TARGET DEVICES contain evidence, instrumentalities, contraband, or fruits of these crimes.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

5. The “TARGET DEVICES” are the following ten electronic devices, which were seized from 721 Faulkner Avenue, Martinsburg, West Virginia, during the execution of a search warrant at that location on January 19, 2023:

- a. Gray-in-color Apple iPhone with cracked screen
- b. Amazon tablet
- c. Acer Chromebook 15
- d. Clear-in-color thumb drive
- e. Apple iPhone in black case
- f. Samsung Galaxy S20 cellular phone
- g. Black Motorola cellular phone
- h. Moto G Stylus cellular phone
- i. Black-in-color Dell laptop computer
- j. Silver-in-color Apple iPhone

6. The TARGET DEVICES are currently stored in the Evidence Room at the FBI, 1250 Edwin Miller Boulevard, Martinsburg, West Virginia, in the Northern District of West Virginia. Based on training and experience, your affiant knows the TARGET DEVICES have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the TARGET DEVICES first came into the FBI's possession.

7. The applied-for warrant would authorize the forensic examination of the TARGET DEVICES for the purpose of identifying the electronically stored information described in Attachment B.

DEFINITIONS

8. The following definitions apply to this affidavit and to Attachment B:

- a. “Cellular telephone” or “wireless telephone” means a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books”; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving videos; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may include geographic information indicating where the cell phone was at particular times.
- b. “Computer”, as used herein, is defined pursuant to Title 18, United States Code, Section 1030(e)(1), as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.”
- c. “Computer hardware”, as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to,

central processing units, laptops, tablets, eReaders, Notes, iPads, and iPods; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, SD cards, thumb drives, flash drives, USB storage devices, CDs and DVDs, and other memory storage devices); peripheral input/output devices (including, but not limited to keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

d. “Computer software”, as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

e. “Computer-related documentation,” as used herein, consists of electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

f. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips,

and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. “Electronic storage devices” includes computers, cellular telephones, tablets, and devices designed specifically to store electronic information (e.g., external hard drives and USB “thumb drives”). Many of these devices also permit users to communicate electronic information through the Internet or through the cellular telephone network (e.g., computers, cellular telephones, and tablet devices such as an iPad).

h. “Tablet,” as used herein, is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

i. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international

borders, even when the devices communicating with each other are in the same state.

j. “Internet Service Providers” (ISPs) are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone-based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an “e-mail address,” an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider (ISP) over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

k. “An Internet Protocol address” (IP address) is a unique numeric address used by Internet-enabled electronic storage devices to access the Internet. Every electronic storage device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that electronic storage device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static— that

is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

l. “Child Pornography,” as used herein, is defined pursuant to Title 18, United States Code, Section 2256(8), as “...any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where – (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.”

m. The term “minor,” as used herein, is defined pursuant to Title 18, United States Code, Section 2256(1), as “any person under the age of eighteen years.”

n. The term “sexually explicit conduct,” as used herein, is defined pursuant to Title 18, United States Code, Section 2256(2) as “actual or simulated—(i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person.”

o. “Visual depictions” include data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See Title 18, United States Code, Section 2256(5).

p. The terms “documents” and “materials” include all information recorded in any form, visual or aural, and by any means, whether in electrical, electronic or magnetic form (including tape recordings, compact discs, electronic or magnetic storage devices such as hard disks, CD-ROMs, digital video disks (DVDs), Multi Media Cards (MMCs), memory sticks, smart cards, or electronic notebooks, as well as digital data files and or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

9. Computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was primarily produced using cameras and film (either still photography or movies). Development and reproduction of the images often required darkroom facilities and a significant amount of skill, and there were definable costs involved with the production of pornographic images. Distribution of child pornography on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls. The development of computers has changed this. Computers, of which “smart” phones are one type, basically serve

four functions in connection with child pornography: production, communication, distribution, and storage.

10. Child pornographers can now transfer photographs from a camera onto a computer readable format with a device known as a scanner. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer using telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

11. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media used in home computers and cellular telephones has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

12. The internet and its World Wide Web afford collectors of child pornography a variety of venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

13. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by internet portals such as Yahoo! and Hotmail, among others. The online portals allow a user to set up an account with a remote computing service that provides email services, as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

14. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (e.g., by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally (e.g., traces of the path of an electronic communication may be automatically stored in many places, such as in temporary files or internet service provider client software, among others). In addition to electronic communications, a computer user's internet activities generally leave traces or "footprints" and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains wireless software, was using an instant messaging service, and when certain files under investigation were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

CHARACTERISTICS OF PERSONS WHO TRAFFIC CHILD PORNOGRAPHY

15. As a result of the above-mentioned training and experience, I have learned the following characteristics are generally found to exist in varying combinations and be true in cases involving offenders who send, cause to be sent, distribute, exhibit, possess, display, transport, manufacture or produce material which depicts minors engaged in sexually explicit conduct. Said material includes, but is not limited to, photographs, negatives, slides, magazines, other printed media, motion pictures, video tapes, books, or similar items stored electronically on computers, digital devices or related digital storage media.

- a. These offenders obtain and/or traffic in materials depicting children engaged in sexually explicit conduct through many sources and by several methods and means. These sources, methods and means include, but are not limited to, the following:
 - i. Downloading via the Internet and other computer networks.
(Web sites, peer to peer file sharing networks, newsgroups, electronic bulletin boards, chat rooms, instant message conversations, e-mail, etc.)
 - ii. Receipt from commercial sources within and outside of the United States through shipments, deliveries and electronic transfer.
 - iii. Trading with other persons with similar interests through shipments, deliveries and electronic transfer.
 - iv. Producing and manufacturing these materials during actual contact with children.
- b. These offenders collect materials depicting children engaged in sexually explicit conduct for many reasons. These reasons include, but are not limited to, the following:
 - i. For sexual arousal and sexual gratification.
 - ii. These offenders use child pornographic materials the same way other people use adult pornography—to feed sexual fantasies.
 - iii. Use as a means of reliving fantasies or actual encounters with the depicted children.

- iv. To lower children's inhibitions - A child who is reluctant to engage in sexual activity with an adult or pose for sexually explicit photographs can sometimes be convinced by viewing other children having "fun" participating in sexual activity. Additionally, peer pressure can have a tremendous effect on children. If other children are involved, the child might be led to believe that the activity is acceptable.
- v. Use as blackmail - Children are often afraid that the illicit pictures and/or motion pictures taken of them will be shown to their friends or family. If the child threatens to tell his or her parents or the authorities, the existence of sexually explicit photographs/motion pictures is often an effective silencer.
- vi. As a commodity for exchange -
 - 1. Some offenders exchange illicit images or videos of children for other child pornographic images or videos.
 - 2. Some offenders send, cause to be sent, distribute, exchange, trade or sell these illicit materials to other people with similar interests as a means of gaining acceptance, status, trust and psychological support from these other persons.
 - 3. Some offenders exchange these illicit materials for means by which to contact other children (i.e. telephone numbers, e-mail addresses, screen names, etc.).

4. The quality and theme of the material often determines its value as a commodity for exchange.

vii. For profit -

1. Some offenders involved in the sale and distribution of child pornography are profiteers and are not sexually interested in children.
 2. Other offenders may begin nonprofit trading, which they pursue until they accumulate certain amounts or types of images, which they then sell to distributors for reproduction in commercial child-pornography magazines or made available on the Internet for downloading.
 3. Others offenders may combine their sexual interests in children with their profit motive. Thus an illicit image of a child taken by a local offender in any community in the United States can end up in a commercial child-pornography magazine or on the Internet with worldwide distribution.
- c. These offenders view their child pornographic materials as valuable commodities, sometimes even regarding them as prized collections. Consequently, these offenders prefer not to be without their child pornographic material for any prolonged time period and often go to great lengths to conceal and protect their illicit collections from

discovery, theft, or damage. To safeguard their illicit materials or digital devices which contain their illicit materials, these people may employ the following security measures:

- i. The use of safes and safe deposit boxes.
 - ii. The use of concealed compartments or concealed rooms within premises or other structures that they occupy or have control of.
 - iii. The use of storage facilities outside their immediate residence (outbuildings, motor vehicles, animal cages, recreational vehicles, vessels etc.).
 - iv. The use of Internet-based data storage services.
 - v. Rental of storage facilities.
 - vi. Recording onto media that contains false, misleading or no title(s).
 - vii. The application of digital security technologies, including, but not limited to, password protection, encryption and steganography.
- d. These offenders may send, cause to be sent, distribute, exhibit, possesses, collect, display, transport, manufacture or produce materials depicting children fully clothed, in various stages of undress or totally nude, in various activities and not necessarily sexually explicit. These materials may include, but not be limited to, photographs, negatives, slides, magazines, other printed media, motion pictures, video tapes,

books, or similar items stored electronically on computers, digital devices or related digital storage media. This material is known as “child erotica.” Although it may not meet the definition of child pornography, it is often probative of an offender’s sexual interest in children and criminal intent. These pictures may be cut out of printed media (magazines, newspapers, books, etc.), downloaded from the Internet or surreptitiously taken or recorded by the offender from afar.

- e. In the case of materials which depict a child in the nude or posed in a sexually suggestive manner, there is a high probability that the child was molested before, during, or after the photo-taking and/or video session because the act of the posing is such a great sexual stimulus for the offender taking the pictures and/or making the videos.
 - i. These materials are used by these offenders as a means of establishing and sustaining fantasy relationships.
 - ii. These photos and/or videos are rarely, if ever, disposed of and are revered with such devotion that they are often kept in close proximity to the offender and occasionally upon the offender’s person and such.
- f. These offenders fear discovery and may maintain and operate their own photographic production and reproduction equipment. This may be as simple as the use of “instant” photo cameras, video equipment or as complex as a completely outfitted photographic studio or photograph development laboratory.

PROBABLE CAUSE

16. On December 16, 2022, your affiant began a child exploitation investigation involving Destiny Somersall (Somersall), also known as Destiny [REDACTED], date of birth [REDACTED] 1982, and Somersall's [REDACTED] [REDACTED], referred to hereinafter as "A.M.," date of birth [REDACTED] 2006. Somersall resides at 721 Faulkner Avenue, Martinsburg, West Virginia 25401, referred to hereinafter as the FAULKNER AVENUE RESIDENCE. The Martinsburg Police Department contacted Somersall at the FAULKNER AVENUE RESIDENCE on October 11, October 12, and October 26, 2022. The Berkeley County Sheriff's Office contacted Somersall at the FAULKNER AVENUE RESIDENCE on December 13, 2022. During A.M.'s child forensic interview, she confirmed that her residence was on Faulkner Avenue in Martinsburg.

17. On December 29, 2022, a child forensic interview of A.M. was conducted in Martinsburg, West Virginia. During the interview, A.M. provided the following information: ^{SND} 3. A.M. knew a man who was Somersall's "sugar daddy." The "sugar daddy" was old, white, heavysset, approximately the same height as A.M., and had very little hair on his head. A.M. knew from Somersall that the "sugar daddy" gave Somersall money. The "sugar daddy" sometimes came over to their house and brought them food. He also paid for Somersall and A.M. to take trips and vacations.

18. Approximately two years ago, Somersall came into A.M.'s bedroom in the early morning hours and told A.M. she needed A.M. to do Somersall a favor. Somersall told A.M. to get undressed, and then Somersall took photographs of A.M.'s unclothed body, including A.M.'s exposed genitals and breasts. Somersall used the cellular telephone she

normally used at that time to take the images. The phone had a black case with sparkles. A.M. thought Somersall sent the photographs to someone for money.

19. On several additional occasions, Somersall provided lingerie for A.M. to wear and took photographs and videos of Somersall wearing the lingerie and exposing her genitals to the camera. Somersall told A.M. specific poses to adopt, including lying on her back with her legs spread apart, and bending over. Somersall took photographs from several angles. Sometimes, A.M. could see the flash of the cellular phone's camera activated. On at least one occasion, Somersall told A.M. to put her finger in her vagina for the photographs, which A.M. did.

20. In approximately Fall 2022, A.M. was at home at the FAULKNER AVENUE RESIDENCE in Martinsburg, West Virginia. A.M.'s friend, whom A.M. knew to be approximately 15 years old, was spending the night at A.M.'s house. Somersall pulled A.M. aside and asked A.M. if she liked the house they lived in and if she wanted to keep living there. A.M. said yes. Somersall said A.M. would need to do her a favor. Somersall said A.M. had to make a video with her friend because Somersall had no other way to pay the rent.

21. Somersall told A.M. to take off her clothes and lay on her bed. Somersall told A.M.'s friend to lick A.M.'s thighs and vaginal area. A.M. and her friend did so. Somersall filmed them with a cellular phone. After filming the video, Somersall, A.M., and her friend got in the car and drove to an automated teller machine. Somersall got out of the car and returned with money. Somersall told them they did a good job.

22. Around the time of A.M.'s 15th birthday (██████████ 2021), Somersall made A.M. have sex with the "sugar daddy" because the normal amount of money he supplied Somersall with was not enough. Somersall drove A.M. to a hotel in Hagerstown, Maryland.

The hotel was near a mall and the word “Suites” was in the hotel’s name. Somersall and A.M. went to a room in the hotel and knocked on the door. Somersall’s “sugar daddy” answered the door and they went in. Somersall told A.M. she had to have sex with the “sugar daddy,” because they needed money, or they would be homeless. The “sugar daddy” licked and bit A.M.’s vaginal area, and penetrated A.M.’s vagina with his fingers and with his penis. Eventually the “sugar daddy” groaned loudly and stopped penetrating A.M. A.M. went to the bathroom and observed a clear liquid leaking from her body. On the ride home from the hotel, A.M. saw Somersall had an envelope full of cash.

23. A.M. had to have sex with the “sugar daddy” at the hotel on several additional occasions. On one such occasion, A.M. saw the “sugar daddy” give Somersall cash in the hotel room after he had sex with A.M. A.M. knew Somersall also used Cash App to receive money from the “sugar daddy.” [I am aware that Cash App is a mobile payment service that allows users to transfer money to one another using a mobile phone application.] A.M. provided Somersall’s Cash App account name as “[REDACTED].” A.M. also had a Cash App account that the “sugar daddy” sent money to directly. A.M. thought her Cash App account name consisted of her first and last name. A.M. recalled the “sugar daddy’s” Cash App account name was something similar to “Hagerstown Sugar Daddy” or contained the words “Hagerstown” and “Daddy.” A.M. also saw paper checks Somersall received from the “sugar daddy.” The checks had the name “John” on them.

24. I am aware of an ongoing child exploitation investigation being conducted by Homeland Security Investigations (HSI). The subject of this investigation is John Wayne Balch, date of birth [REDACTED]. Balch is a white male, 75 years old, approximately 5’7”, heavysset, and bald. Based upon commercial databases, law enforcement records, and the HSI

investigation, your affiant is aware that Balch resides in Florida and has previously lived in Maryland.

25. Your affiant reviewed license plate reader (LPR) data from January 2021 through December 2022 for one of Balch's registered license plates, Florida license plate number IQII64. Your affiant located twenty-eight dates during this time frame when vehicles bearing this license plate were recorded near hotels close to the Valley Mall in Hagerstown, Maryland. In most of the photographs captured by the LPRs, it is evident that the vehicle was parked in a parking lot when the license plate was read. The hotels include the Home2Suites hotel and Homewood Suites hotel.

26. HSI agents collected records associated with Balch's Cash App account. Cash App is a payment service offered by Block, Inc., of San Francisco, California. As noted above, Cash App can be used as a peer-to-peer payment service, meaning individuals can connect directly to each other to exchange money through the Cash App mobile application. In order to transfer money, a user can use existing funds in their Cash App account or fund the transfer through a linked credit card account. A user can create a unique alpha-numeric name, known as a "cashtag" for identification purposes. Users can also add a display name, such as first and last name, and a profile photograph to their accounts as further identification. One of Balch's cashtags identified during the HSI investigation was "Hagerstowndaddy." An analysis of Balch's Cash App account revealed that between November 2, 2020 and November 8, 2022, there were sixty outgoing transactions from Balch's Cash App account to a Cash App account bearing the name "Destiny Somersall," a profile photograph of Somersall, and the cashtag "[REDACTED]." These sixty transactions totaled \$13,725. HSI also recovered evidence of at least eleven Cash App payments from Balch to a Cash App account with the name "[REDACTED]"

██████” and cashtag “██████” between November 24, 2020 and August 20, 2022, totaling \$2,375. Further analysis of the Cash App records is ongoing.

27. On January 19, 2023, law enforcement agents executed a search warrant on the FAULKNER AVENUE RESIDENCE and seized the TARGET DEVICES from within the residence. Just prior to the execution of the search warrant, your affiant made contact with Somersall at the FAULKNER AVENUE RESIDENCE. Your affiant interviewed Somersall after providing her Miranda rights, and Somersall provided the following information:

28. Somersall had known John Balch for several years and Balch had paid her for sexual activity. Balch told Somersall he would pay her money for sexual images of A.M. including images of A.M. masturbating and A.M. posing in lingerie. Somersall took and sent such images to Balch in exchange for money, using her cellular phone and A.M.’s cellular phone. Somersall sent Balch the images via text message and via a mobile texting application. Some of the images were taken at the FAULKNER AVENUE RESIDENCE and others were taken in Somersall’s previous residence. Somersall sent the images to Balch via text message and a mobile texting application. Somersall estimated she began taking such pictures of A.M. one or two years ago. Balch sent money to Somersall via CashApp and by check.

29. Somersall advised that on two to three occasions, she transported A.M. to a hotel near the Valley Mall in Hagerstown for sex with Balch in exchange for money. Somersall estimated that the first time was around Christmas 2021 (before Christmas) and the last time was Summer 2022.

30. On each occasion, Somersall advised she performed oral sex on Balch, and then Balch had vaginal sex with A.M. The first time, Balch immediately paid A.M. \$3,000

cash placed in a bank envelope and he also paid Somersall \$4,000 in cash plus \$1,000 via check. She advised Balch also took them to buy cellular phones, as he had promised to buy A.M. a phone in exchange for sex. Somersall thought the hotel was possibly a Home2Suites hotel in Hagerstown, MD.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

31. Based on my training, experience, and research, I know the TARGET DEVICES have capabilities that allow them to serve as wireless telephones, computers tablets, and electronic storage devices.

32. Based on my knowledge, training, and experience, I know electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the devices. This information can sometimes be recovered with forensics tools.

33. There is probable cause to believe that things that were once stored on the TARGET DEVICES may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file

does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

34. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct

evidence of the crimes described on the warrant, but also forensic evidence that establishes how the TARGET DEVICES were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the TARGET DEVICES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a device can also indicate who has used or controlled the devices. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

35. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the TARGET DEVICES consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that

might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

36. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

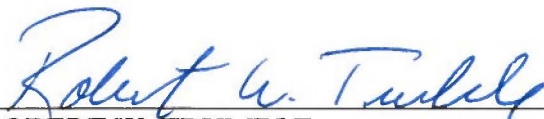
37. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the TARGET DEVICES described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



Ellen Duffy, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on January 25, 2023.



ROBERT W. TRUMBLE
UNITED STATES MAGISTRATE JUDGE